LA ELABORACIÓN DE PERFILES Y SU IMPACTO EN LOS DERECHOS FUNDAMENTALES. UNA PRIMERA APROXIMACIÓN A SU REGULACIÓN EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA

PROFILE DEVELOPMENT AND ITS IMPACT ON FUNDAMENTAL RIGHTS. A FIRST APPROXIMATION TO ITS REGULATION BY THE GENERAL DATA PROTECTION REGULATION OF THE EUROPEAN UNION

Ana Garriga Domínguez
Universidad de Vigo

Fecha de recepción: 15-7-16
Fecha de aceptación: 8-3-17

Resumen: *En la sociedad de los datos masivos y de la computación ubicua la elaboración de perfiles, cada vez más precisos, para la adopción de decisiones sobre personas y su clasificación, puede suponer claros riesgos a los derechos fundamentales de las personas y su dignidad. En este contexto, se analiza su regulación en el nuevo Reglamento General de Protección de Datos de la Unión Europea.*

Abstract: *In the society of Big Data and ubiquitous computing, decisions based on profiling can pose significant risks to the fundamental rights and human dignity. In this context, regulation is analysed in the new General Data Protection Regulation of the European Union.*

Palabras clave: privacidad, perfilado, Big Data, computación ubicua, Unión Europea
Keywords: privacy, profiling, Big Data, ubiquitous computing, European Union

1. DATOS MASIVOS, COMPUTACIÓN UBICUA, SERVICIOS ONLINE E INTERNET DE LAS COSAS

Hace más de una década, Lawrence Lessing auguraba que Internet se convertiría en *"un espacio de control ejercido, en su mayor parte, por las tecnologías del comercio respaldadas por las reglas que impone la ley"*[1]. Lo cierto es que, como consecuencia lógica del progreso de la tecnología informática, se ha operado un espectacular desarrollo de Internet acompañado de un vertiginoso incremento del número y clase de servicios disponibles a través de la red usados por millones de personas. Esta interacción en la red va a ser seguida y analizada por diversos *vigilantes*, que por diferentes razones e intereses, recogen y observan nuestra actividad en los distintos servicios y redes de la Sociedad de la Información. En el mundo de la vigilancia líquida[2] cada uno de nuestros comentarios, acciones o intereses es susceptible de pasar a engrosar alguno de los muchos centros de datos personales que los Estados y las entidades privadas poseen y que en numerosas ocasiones constituyen su activo y objeto de negocio principal.

Como consecuencia de las posibilidades de seguimiento de la actividad en la red y de la proliferación de tecnologías que permiten la localización y la monitorización de la actividad humana en tiempo real, nuestro mundo puede calificarse con acierto como sociedad del control[3] o sociedad de la transparencia[4] y, por el conjunto de actividades que se desarrollan derivadas de la incesante infiltración de las tecnologías de la información y la comunicación (TIC) en nuestras vidas, no resulta exagerado en algunos casos hablar de posibilidades de vigilancia masiva o vigilancia total.

Debemos tener presente que con Internet se ha generalizado la recogida y tratamiento de enormes cantidades de información sobre personas. Datos que provienen, no sólo de los que nosotros facilitamos directamente a través de la información que voluntariamente subimos a la red, sino también de los rastros que dejamos de forma inconsciente. La navegación por Internet gene-

---

[1] L. LESSING, *El código y otras leyes del ciberespacio,* traducción de E. Alberola, Taurus, Madrid, 2001, p. 12.

[2] Z. BAUMAN y D. LYON, *Vigilancia líquida,* traducción de Alicia Capel Tejer, Paidós, Barcelona, 2013.

[3] G. DELEUZE, *"Postscript on the Societies of Control"*, vol. 59., 1992, p. 3-7. Puede consultarse en: *http://links.jstor.org/sici?sici=0162-2870%28199224%2959%3C3%3APOTSOC%3E2.0.CO%3B2-T.*

[4] H. BYUNG-CHUL, *La sociedad de la transparencia,* traducción de Raúl Gabás, Herder, Barcelona, 2013.

ra gran cantidad de datos transaccionales de forma que cuando se accede a la red se deja un rastro digital y, *"al ser cada vez mayor el número de actividades de nuestro quehacer cotidiano que se realizan el línea, irá aumentando la información que sobre nuestras ocupaciones, gustos y preferencias quede registrada"*[5]. A través de «cookies remotas» o programas rastreadores se posibilita el funcionamiento de las denominadas «*redes de seguimiento*» mediante las que es posible seguir al usuario a medida que navega por determinados «*sitios*», *"vigilando sus acciones, acumulando información personal, controlando cuales bienes o servicios adquiere, etc."*[6]. Este rastro podrá reunirse e interrelacionarse, con la consiguiente *"transformación de datos en principio irrelevantes en un perfil peligrosamente público del ciudadano"*[7], ya que existen soportes lógicos capaces de buscar y recopilar todos los datos que sobre una misma persona se encuentren en la red[8]. La problemática derivada del tratamiento de este tipo de datos personales se complica también por que se trata de «datos invisibles» para el usuario, cuyo almacenamiento o elaboración escapan a su conocimiento y a su control[9] y porque Internet implica *"el riesgo de un efecto multiplicador de los atentados contra derechos, bienes e intereses jurídicos"*[10].

Igualmente, la digitalización en nuestra forma de comunicarnos e interactuar con otras personas, especialmente con la aparición de la web 2.0 ha tenido un impacto considerable a este respecto. La desaparición de las nociones de espacio y el tiempo en la comunicación[11], las posibilidades de inmediatez en la transmisión de toda clase de actos, pensamientos, imágenes o emociones van a tener consecuencias, a veces inesperadas, para quienes se expresan en la red. Cada individuo puede ser emisor y difusor de informa-

---

[5] Recomendación 3/97, del Grupo de Trabajo del Artículo 29 (GT 29).

[6] A. TÉLLEZ AGUILERA, *Nuevas tecnologías, intimidad y protección de datos*, Edisofer, Madrid, 2001, p. 83.

[7] V. DRUMMOND, *Internet, privacidad y datos personales*, traducción de I. Espín Alba, Editorial Reus, Madrid, 2004, p. 118.

[8] Vid. El documento de trabajo sobre *Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea*, adoptado el 21 de noviembre de 2000, del Grupo de Trabajo del artículo 29.

[9] Vid. Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware, aprobada por el Grupo de Trabajo el 23 de febrero de 1999.

[10] A. E. PÉREZ LUÑO, *La tercera generación de derechos humanos,* Thomson Aranzadi, Navarra, 2006, p. 93.

[11] H. CAMPUZANO TOMÉ, *Vida privada y datos personales. (Su protección jurídica frente a la sociedad de la información),* Tecnos, Madrid, 2002, p. 17.

ción a través de las redes sociales, foros, blogs y bitácoras, que será expresada mediante textos, sonidos o imágenes propios y de terceros, acompañadas de valoraciones, descripciones y opiniones. Con la proliferación de herramientas de comunicación y de expresión, *"habida cuenta de la posibilidad de «remixaje» y de bricolaje de todo lo que existe",* cada vez son mayores las posibilidades de reelaboración y descontextualización de esa información que los usuarios hacen disponible[12].

Otra consecuencia de nuestra interacción *online* es la mezcla entre lo público y lo privado, ya que el medio digital *privatiza* la comunicación en la medida en que *"desplaza de lo público a lo privado la producción de información"*[13]. La comunicación digital fomenta una enorme exposición de la vida personal de un gran número de personas, en especial a través de las redes sociales. Incluso desde antes de su nacimiento algunas personas tienen presencia en la red, por ejemplo, a través de las ecografías que publican sus padres[14]. La comunicación digital *"fomenta esta exposición pornográfica de la intimidad y de la esfera privada"*[15] y unida a factores como la despreocupación y descontextualización de la información subida a la red, puede suponer que nuestra *"trayectoria vital grabada en la red, se vea hipotecada por el recuerdo constante"* del pasado, especialmente en el caso de los más jóvenes[16]. Además, la proliferación de dispositivos conectados para realizar toda clase de actividades en la red ha tenido como consecuencia que hoy nos encontramos, respecto de la cantidad de información personal disponible, ante una nueva revolución tecnológica que *"no se cifra en las máquinas que calculan los datos, sino en los*

---

[12] C. COBO ROMANÍ y H. PARDO KUKLINSKI, *Planeta Web 2.0. Inteligencia colectiva o medios fast food*, Grup de Recerca d'Interaccions Digitals, Universitat de Vic -Flacso México, 2007, Barcelona / México DF, p. 21.

[13] H. BYUNG-CHUL, *En el enjambre,* traducción de Raúl Gabás, Herder Editorial, Barcelona, 2014, p. 14.

[14] El 81% de los niños de menos de dos años tiene alguna forma de presencia en Internet, el 7% de los bebés y niños pequeños tiene una cuenta de correo electrónico creada para ellos (en España este porcentaje sube al el 12%) y el 5% tiene su propio perfil en redes sociales. En Informe *"Digital Birth: Welcome to the Online World",* Informe elaborado por AVG Technologies, según el cual aproximadamente una cuarta parte de los niños del mundo tienen presencia en Internet antes de su nacimiento. Puede consultarse en:

http://www.businesswire.com/news/home/20101006006722/en/Digital-Birth-Online-World#.VVHUHjfDHyI.

[15] H. BYUNG-CHUL, *En el enjambre*, cit, p. 14.

[16] P. SIMÓN CASTELLANO, *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch - Agencia Española de Protección de Datos, Valencia, 2012, p. 39.

datos mismos y en cómo los usamos"[17]. Es decir, no sólo es relevante a efectos del rastro digital, el tipo de información que ponemos a disposición de otros en Internet, sino que otro factor importantísimo es el de su cantidad, que va suponer por sí mismo un nuevo tipo de riesgo para los derechos.

La cantidad de datos personales que hay en todo el mundo comienza a ser difícil de cuantificar y aumenta cada minuto del día. Nuestra forma de usar la red y muchos de los servicios disponibles tiene como consecuencia directa un continuo aporte de información sobre nosotros mismos. Tras un año de visitas a la red *"la incansable maquinaria de registrar metadata ha acumulado miles de páginas sobre nosotros en un archivo que incluye nuestro nombre, dirección, estado civil, financiero y emocional; compras, viajes, amigos, inclinaciones políticas y predicciones acerca de nuestras vidas basadas en todo lo anterior"*[18]. Los millones de usuarios de los diferentes servicios en Internet generan enormes cantidades de información sobre ellos y sobre terceros cada vez que los utilizan[19].

En la era de los grandes datos, éstos se ha convertido en la materia prima, en una nueva fuente de inmenso valor económico y social. Los avances en la minería y análisis de datos y el aumento masivo de la capacidad informática de procesamiento y almacenamiento de datos se han ampliado exponencialmente y la información se encuentra al alcance de las empresas, los gobiernos y los individuos. Igualmente, el número creciente de personas, dispositivos y sensores que están conectados por redes digitales ha revolucionado la capacidad de generar, comunicar, compartir y acceder a los datos[20].

---

[17] V. MAYER-SCHÖNBERGER y K. CUKIER, *Big data. La revolución de los datos masivos,* Turner Noema, 2013, p. 18.

[18] M. PEIRANO, *El pequeño libro rojo del activista en la red,* eldiario.es libros - Roca editorial, segunda edición, Barcelona, 2015, p. 25.

[19] La cantidad de datos desde 2014 se ha multiplicado y no dejará de aumentar en los próximos años. Según el estudio Big Data 2015 de OBS Business School, *"en un minuto, en Internet se generan 4,1 millones de búsquedas en Google, se escriben 347.000 twitts, se comparten 3,3 millones de actualizaciones en Facebook, se suben 38.000 fotos a Instagram, se visualizan 10 millones de anuncios, se suben más de 100 horas de vídeo a Youtube, se escuchan 32.000 horas de música en streaming, se envían 34,7 millones de mensajes instantáneos por Internet o se descargan 194.000 apps."* Además, se calcula que en 2020 habrá más de 30 mil millones de dispositivos conectados a la red. En *http://www.obs-edu.com/noticias/estudio-obs/en-2020-mas-de-30-mil-millones-de-dispositivos-estaran-conectados-internet/.*

[20] O. TENE y J. POLONETSKY, "Privacy in the age of Big Data: a time for big decisions*", Stanford Law Review Online,* num. 63, 2012, p. 63.

Puede consultarse *en https://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf.*

Las posibilidades de análisis estadístico y predictivo de los datos en la era de los datos masivos son difíciles de imaginar, *"al cambiar la cantidad cambiamos la esencia"*, pues al emplear todos los datos disponibles podemos apreciar *"detalles que nunca pudimos ver cuando estábamos limitados a las cantidades más pequeñas"*[21]. Hoy, señalan Craig y Ludloff, han desaparecido la barreras tradicionales para el análisis de los grandes conjuntos de datos y que históricamente habían retenido la ciencia de minería de datos y los modelos de predicción, ya que la tecnología contemporánea posibilita el almacenamiento y el procesamiento posterior de ingentes cantidades de datos a un coste relativamente barato[22].

El término Big Data hace referencia a dos cuestiones íntimamente relacionadas. En primer lugar, a la gran cantidad de datos disponibles, es decir, a la existencia de un masivo volumen de datos que pueden ser utilizados con diversos fines. En segundo lugar, se alude también al conjunto de tecnologías, *"que pertenecen al campo de la inteligencia artificial (y) recibe el nombre de «minería de datos»"*[23] y cuyo objetivo es tratar grandes cantidades de información[24] empleando complejos algoritmos y estadística con la finalidad de hacer predicciones, extraer información oculta o correlaciones imprevistas y, en último término, favorecer la toma de decisiones. Así pues, cuando utilizamos la expresión Big Data nos estamos refiriendo, por una parte, a la ingente cantidad de datos, disponibles y, por otra al conjunto de herramientas y sistemas informáticos que analizan los datos buscando patrones recurrentes y correlaciones dentro del conjunto de aquellos.

Asimismo, el Big Data puede ser definido como un fenómeno cultural, tecnológico y académico, que se apoya en la interacción de la tecnología a través de la maximización de la potencia de cálculo y precisión algorítmica para reunir, analizar, vincular y comparar grandes conjuntos de datos, pero que, en último término, aportaría un elemento mitológico, entendido como la creencia generalizada de que los grandes conjuntos de datos ofrecen una forma superior de la inteligencia y que su conocimiento puede gene-

[21] V. MAYER-SCHÖNBERGER y K. CUKIER, *Big data. La revolución de los datos masivos,* cit., p. 22 y 25.

[22] T. CRAIG y M. E. LUDLOFF, *Privacy and Big Data,* O'Really, 2011, Sebastopol (California), p. 5.

[23] A. RAMOS BERNAL, *Reflexiones sobre economía cuántica,* ECU (editorial Club Universitario), Alicante, 2012, p. 186.

[24] Vid. M. BELTRÁN PARDO y F. SEVILLANO JAÉN, *Cloud computing, tecnología y negocio,* Paraninfo, Madrid, 2013, p. 16 y ss.

rar ideas que antes eran imposibles, con el aura de la verdad, la objetividad y la precisión[25]. Ahora bien, no siempre estamos ante una tecnología neutra, los Big Data pueden manipularse ya que *"las estadísticas lo saben todo sin demostrar nada, son pruebas aparentemente científicas de presupuestos altamente ideológicos"*[26].

Los datos no provienen solamente de nuestra interacción en la red, una gran cantidad de ellos, que cada vez serán más numerosos en el futuro, serán obtenidos gracias al *"Internet de las cosas",* puesto que cada vez hay más dispositivos conectados a Internet generando información de forma constante. Cuando se habla de Internet de las cosas se hace referencia a un conjunto de objetos cotidianos conectados digitalmente a Internet entre los que debe existir *"algún tipo de intercambio de información para que esos objetos representados por la palabra 'cosas' trabajen en el mundo de los datos"*[27]. Es decir, no se trata de que un objeto cotidiano, por ejemplo un electrodoméstico, cuente con un software integrado sino que, lo que lo convierte en parte del mundo de Internet de las cosas, es que recopila información sobre el uso que hacemos de ese objeto y la transforma en datos que procesa y envía a Internet.

Dentro del Internet de las cosas, son cada vez más numerosos un tipo de objetos que pertenecerían a la categoría de los denominados «wearables» o "tecnología vestible", como calzado, relojes y pulseras inteligentes o las "google glass", los relativos a la domótica o los denominados sensores portátiles y el conjunto de dispositivos y aplicaciones para registrar y procesar datos sobre nuestros hábitos cotidianos, número de pasos, calorías que quemamos, temperatura de nuestro cuerpo, pautas de sueño, entrenamiento deportivo, etc.[28] Para incluirlos en la categoría de Internet de las cosas, estos dispositivos deben tener poder de cálculo y estar conectados a sensores

---

[25] D. BOYD y K. CRAWFORD, "Critical questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon", *Information, Communication & Society*, vol. 15, núm. 5, 2012, p. 662 y 663.

[26] IPPOLITA, *En el acuario de Facebook. El irresistible ascenso del anarco-capitalismo*, traducción de Guiseppe Maio, Enclave de Libros, Madrid, 2012, p. 106.

[27] A. McEWEN y H. CASSIMALLY, *Internet de las cosas. La tecnología revolucionaria que todo lo conecta*, Anaya Multimedia, Madrid, 2014, p. 27.

[28] Vid. entre otros, M. SWAN, "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0", *Journal of Sensor and Actuator Netwowoks*, num. 1 vol. 3, p. 217-253, 2012 (puede consultarse en *http://www.mdpi.com/2224-2708/1/3/217/htm*). También, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, del Grupo de Trabajo sobre protección de datos del artículo 29, adoptado el 16 de septiembre de 2014.

electrónicos, que interactúen con el mundo real y que, finalmente, habrán de estar conectados a Internet[29]. El elemento diferenciador de éstos con otro tipo de dispositivos es su capacidad de compartir y procesar información con otros servicios o con otros usuarios[30]. Se trata de dispositivos que pueden acompañar a una persona desde el mismo momento de su nacimiento, como los monitores para bebés que se colocan como una tobillera y miden la temperatura, la frecuencia cardiaca, sus movimientos durante el sueño, la temperatura y la luz de la habitación y están sincronizados al Smartphone para enviar toda la información[31].

Otra clase de tecnologías cuyo uso está muy extendido son los dispositivos de geolocalización. Lo forman una gran variedad de sistemas que localizan con precisión la posición geográfica de un objeto determinado y, de manera asociada, de una persona concreta. Son muchos los servicios que recogen y procesan datos de localización geográfica[32], entre los que ocupan un lugar destacado por su potencial invasivo en la privacidad de sus portadores el conjunto de servicios de geolocalización disponibles en dispositivos móviles inteligentes, como nuestros Smartphone. La tecnología de geolocalización puede llegar a revelar detalles íntimos sobre la vida privada al permitir a los proveedores de estos servicios *"una visión personal de los hábitos y patrones del propietario del dispositivo"* y de esta forma elaborar perfiles exhaustivos incluso con datos sensibles como visitas a hospitales o lugares de culto y, todo ello, sin que el interesado sea consciente de que está enviando su ubicación, ni de a quién lo hace o para qué la envía[33]. Igualmente muchos de los dispositivos que forman parte de Internet de las cosas transmiten información sobre su situación geográfica. Los coches pueden comunicar su ubicación a través de sistemas GPS, por ejemplo para evitar robos. Estos datos se pueden combinar con otros y a través de la conexión a Internet de los vehículos además de enviar datos se puede dialogar con un servicio externo con el fin de encontrar la ruta con me-

[29] M. SWAN, *"Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0*, cit., p. 29.

[30] Ibídem.

[31] Vid. *La era del "bebé data"* por Karelia Vázquez, publicado por periódico el país el 1 de mayo de 2015. Puede consultarse en:
http://tecnologia.elpais.com/tecnologia/2015/05/01/actualidad/1430498554_319713.html.

[32] Vid. Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, del Grupo de Trabajo sobre protección de datos establecido por el artículo 29, adoptado el 16 de mayo de 2011, p. 3.

[33] Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, del Grupo de Trabajo del artículo 29, adoptado el 16 de mayo de 2011.

nos tráfico. Pero, cuando se envían los datos internos del vehículo a Internet ya es posible procesarlos, analizarlos, combinarlos y mezclarlos con otras fuentes de información, abriéndose *"un sinfín de posibilidades y ni siquiera somos capaces de imaginar muchas de ellas"*[34]. Por ejemplo, a través del seguimiento constante de nuestra posición geográfica se puede inferir el lugar en el que está nuestro domicilio, nuestro trabajo, si vamos mucho o poco al gimnasio, si nos mudamos de casa, etc. El potencial de esta información *"es enorme, desde la perspectiva del marketing, pues con la misma se podrían ofrecer productos o servicios"*[35], propios o de terceros sobre todo en los casos en los que el geomarketing se desarrolle *"en áreas delimitadas o regiones locales"*[36].

Las tecnologías descritas, son sólo una muestra de las que existen en la actualidad y que se verán incrementadas en el futuro a través del mayor número de dispositivos domésticos conectados, implantados en el cuerpo de las personas (suministradores de medicamentos, marcapasos o prótesis con sensores que recogen y transmiten información médica relevante) y las infinitas aplicaciones de la tecnología «vestible». Igualmente, la evolución de la microelectrónica, y actualmente de la nanotecnología, permite *"diseñar todo tipo de sensores para medidas físicas y químicas, y cada vez más también biológicas, con buena resolución y fiabilidad y a un coste cada vez menor"*[37]. Todos estos sensores cada vez más extendidos y generalizados proporcionarían un gran volumen de datos *"útil para entender diferentes modelos físicos, sociales o económicos"*[38]. Por último, también las iniciativas sobre *Smart Cities*[39], contribuirán de forma notable a incrementar la cantidad de datos disponibles.

El conjunto de tecnologías existentes formarían una red ubicua caracterizada por *"una activación automática de conexiones entre objetos equipados con*

---

[34] A. McEWEN y H. CASSIMALLY, *Internet de las cosas. La tecnología revolucionaria que todo lo conecta*, cit., p. 30.

[35] D. LÓPEZ JIMÉNEZ y E. C. DITTMRA,*"Internet móvil y geolocalización: nuevos retos para la privacidad en la era digital"*, en J. VALERO TORRIJOS, *La protección de los datos personales en Internet ante la innovación tecnológica,* Aranzadi, Cizur Menor, 2013, p. 526 y 527.

[36] Ibídem.

[37] *Big Data en los Entornos de Defensa y Seguridad*, Documento resultado del Grupo de Trabajo sobre Big Data, de la Comisión de Investigación de Nuevas Tecnologías del Centro Superior de Estudios de la Defensa Nacional (CESEDEN), Documento de Investigación 03/2013 Instituto Español de Estudios Estratégicos, p. 9. Puede consultarse en: *http://www.ieee.es/Galerias/fichero/docs_investig/DIEEEINV032013_Big_Data_Entornos_DefensaSeguridad_CarrilloRuiz.pdf.*

[38] Ibídem, p. 10.

[39] Ibídem.

sensores o etiquetas inteligentes, capaces de detectarse y entrar en comunicación"[40]. Esta recolección de datos omnipresente se caracteriza por su falta de visibilidad y transparencia motivada por diversos factores: el propio diseño de la tecnología, que busca ser intuitiva y le resta control al usuario y la multitud de actores e intermediarios involucrados, tanto del ámbito público como privado. De esta forma cada vez estará menos claro quién tiene el control de los datos y quién tiene acceso a ellos con la consiguiente falta de transparencia[41].

La recolección de grandes conjuntos de datos y su posterior análisis bajo las herramientas del Big Data tiene un impacto directo el conjunto de derechos que garantizan la privacidad de las personas y generan nuevas preocupaciones. Las tareas de garantizar la seguridad de los datos y la protección de la privacidad se vuelven más difíciles cuando la información se multiplica y se comparte cada vez más ampliamente en todo el mundo. La información financiera, sobre compras, relativa a la salud, ubicación geográfica, la que se obtiene a través de las tarjetas de fidelización, el uso que cada persona hace de la electricidad y su actividad en línea, está expuesta al escrutinio, público y posibilita la realización de perfiles con el consiguiente riesgo de discriminación o exclusión y, evidentemente, supone la más absoluta pérdida de control de cada individuo sobre su información personal. Si bien nos parece que muchos de los datos son invisibles y parecen impersonales, la realidad es bien distinta: casi cualquier tipo de datos se puede utilizar, de forma similar a una huella digital, pues *"cuantos más datos haya, menos se puede decir que sean privados, ya que la riqueza de dichos datos hace que la localización de personas sea 'algorítmicamente posible'"*[42].

Incluso el propio concepto de dato personal[43] debería empezar a cuestionarse. En el contexto actual, *"la información puede vincularse y desvincularse de una persona conforme pasa el tiempo, en relación con los distintos actores y en*

[40] Mª. R. LLÁCER MATACÁS, "La autodeterminación informativa en la sociedad de la vigilancia: Ubiquitous Computing", en Mª. R. LLÁCER MATACÁS (coord.), *Protección de datos personales en la sociedad de la información y la vigilancia,* La Ley, Madrid, 2011, p. 62.

[41] B. W. SCHERMER, *Surveillance and Privacy in the Ubiquitous Network Society*, Amsterdam Law Forum, vol. 1, num. 4, Septiembre de 2009, especialmente p. 68 y ss. Puede consultarse en: *http://ssrn.com/abstract=1509360.*

[42] P. TUCKER, "*¿Han hecho los grandes volúmenes de datos que el anonimato sea imposible?"*, MIT Technology Review, 16 de mayo de 2013, traducción de Francisco Reyes (OPINNO). Puede consultarse en: *https://www.technologyreview.es/negocios/43072/han-hecho-los-grandes-volumenes-de-datos-que-el/.*

[43] Sobre el concepto de dato personal vid. Dictamen del Grupo de Trabajo 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio de 2007.

los diferentes contextos, dependiendo de su uso y de la manera que se enriquece con datos secundarios"[44].

Una de las herramientas más poderosas para predecir comportamientos personales son la búsqueda y el análisis de las correlaciones hasta el punto de que se afirma que *"las predicciones basadas en correlaciones son el corazón de los datos masivos"*[45]. La era del Big Data es la era de los grandes volúmenes de datos, pero es, sobre todo la época en la que el conjunto de herramientas tecnológicas disponible cuenta con una inmensa capacidad para buscar, agregar y realizar referencias cruzadas de esos grandes conjuntos de datos[46], que permitirá extraer patrones de comportamiento y perfiles personales. A través de nuestro rastro digital se obtienen multitud de datos que, combinados, permiten extraer diversos perfiles que informan acerca de lo que somos y lo que hacemos[47].

La información se ha transformado en un bien básico para las sociedades y para el funcionamiento de la economía y *"la concentración de las fuentes que generan esta información indica que la acumulación del poder económico, lejos de estar disminuyendo se está acentuando"*[48]. Esos cambios producidos por la proliferación de servicios en la red hace necesario que las normas que aseguran el derecho a la protección de datos personales presten una especial atención a las relaciones de las personas con el sector privado[49]. Empresas privadas que ofrecen, por ejemplo, dos de los servicios más populares en Internet, con millones de usuarios cada día: los buscadores y las redes sociales. Tanto unos como otros pueden suponer una gran impacto en los derechos de las personas, a través del rastro digital, que permite monitorear las actividades de las personas en la red para completar con datos obtenidos por otras vías completar su perfil[50]. Los motores de búsqueda *"nos siguen y almacenan enor-*

---

[44] H. GRAUX, J. AUSLOOS y P. VALCKE, *"El derecho al olvido en la era de Internet"*, en J. PÉREZ y E. BADÍA, *El debate sobre la privacidad y la seguridad en la Red: regulación y Mercados,* Ariel- Fundación Telefónica, Barcelona, 2012, p. 117.

[45] V. MAYER-SCHÖNBERGER y K. CUKIER, *Big data. La revolución de los datos masivos,* cit., p. 75.

[46] D. BOYD y K. CRAWFORD, *Critical questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon*, cit., p. 662.

[47] T. CRAIG y M. E. LUDLOFF, *Privacy and Big Data*, cit., p.6.

[48] F. BADÍA, *Internet: situación actual y perspectivas*, Colección Estudios Económicos, num. 28, La Caixa, Barcelona, 2002, p. 29.

[49] C. BENNETT y C. D. RAAB, *The governance of privacy. Policy Instruments in Global Perspective,* The MIT Press, Massachusetts, 2006, p. 269.

[50] H. TAVANI, *Privacy online, Computers and Society* Homepage archive, vol. 29, diciembre de 1999, ACM, New York, p. 11-19.

mes cantidades de información sobre nosotros"[51], sin que seamos conscientes de ello y, por otro lado, informaciones que antes estaban dispersas y que eran difíciles de encontrar, son ahora fácilmente accesibles a través del uso de los medios de búsqueda automatizada de Internet[52].

Los buscadores tratan datos personales que les permite contextualizar las búsquedas con el objetivo optimizarlas y orientar la publicidad que generalmente acompaña a éstas y de la que depende la rentabilidad de los prestadores de este tipo de servicio. Como ha señalado el Tribunal de Justicia de la Unión Europea en relación con Google, los motores de búsqueda, *"al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica"*, recogen datos personales *"que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores y, en su caso, «comunica» y «facilita el acceso» a sus usuarios en forma de listas de resultados de sus búsquedas"*[53]. De esta forma, señala el Tribunal de Justicia,

> *"un tratamiento de datos personales como el controvertido en el litigio principal, efectuado por el gestor de un motor de búsqueda, puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales cuando la búsqueda realizada sirviéndose de ese motor de búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o sólo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o*

[51] A. SUÁREZ OCAÑA, *Desnudando a Google. La inquietante realidad que no quieren que conozcas,* Planeta, Barcelona, 2012, p. 253 y ss.

Así lo ha señalado en su Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda, de 4 de abril de 2008, el Grupo de Trabajo sobre Protección de Datos del artículo 29. En los últimos años se ha producido un aumento de las denuncias de particulares contra este tipo de servicios, poniéndose de manifiesto que "*las capacidades de representación y agregación de los motores de búsqueda pueden perjudicar considerablemente a los individuos, tanto en su vida personal como en la sociedad, en particular si los datos personales que figuran en los resultados de la búsqueda son incorrectos, incompletos o excesivos*".

[52] H. TAVANI, *"Privacy and the Internet"*, en M. M. PLASENCIA, *Privacy and the Constitution,* Garland Publishing, Inc., New York, 1999, p. 266.

[53] Sentencia de 13 de mayo de 2014 (Asunto C-131/12).

> *menos detallado de la persona de que se trate. Además, el efecto de la injerencia en dichos derechos del interesado se multiplica debido al importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo.*"

Los usos de esta información pueden ser varios. Por ejemplo Google, *"a partir de los terabytes de datos sobre comportamiento humano que recogen con su motor de búsqueda y otros sitios web (…) lleva a cabo millones de experimentos diarios, cuyos resultados utiliza para afinar sus algoritmos, que guían cada vez más nuestra manera de encontrar información y de extraer significado de ella"* [54]. Otros usos posibles son las de ofrecer publicidad a medida del usuario en función de sus intereses y preferencias detectadas a partir de su rastro digital. Este cruce de datos puede ofrecer un perfil complejo del usuario, en el que el prestador del servicio podría estar *"a un paso de la ilicitud, principalmente tratándose de la posibilidad de comercialización de datos personales"* [55].

En el caso de las redes sociales, en la medida en que se trata de servicios que ofrecen medios de interacción entre los usuarios basados en los perfiles que éstos mismos generan, formándose comunidades de personas que comparten determinados intereses (profesionales, sobre actividades o aficiones, etc.), a la información personal publicada en línea por el propio usuario, debe añadirse la relativa a sus acciones e interacciones. El usuario de las redes sociales asume un doble papel, el de consumidor y el de creador y, de esta forma *"son los propios usuarios los que crean una gran base de datos cualitativos y cuantitativos, propios y ajenos con información relativa a edad, sexo, localización e intereses"* [56]. La combinación de estos datos que el usuario aporta sobre el mismo y sobre terceros permite la obtención de un perfil muy preciso de sus intereses y actividades.

En las redes sociales aceptamos como «amigos», no sólo a nuestros familiares y amigos, sino a simples conocidos o incluso a completos desconocidos perdiendo el control sobre quien tiene acceso a la información

---

[54] N. CARR, *¿Qué está haciendo Internet con nuestras mentes? Superficiales,* traducción de Pedro Cifuentes, Taurus Pensamiento, Madrid, 2011, p. 184 y 185.

[55] V. DRUMMOND, *Internet, privacidad y datos personales,* cit., p. 118.

[56] P. ORTIZ LÓPEZ, *"Redes sociales: funcionamiento y tratamiento de información personal"*, en A. RALLO LOMBARTE y R. MARTÍNEZ MARTÍNEZ (coord.), *Derecho y redes sociales*, Civitas, Madrid, 2010, p. 24.

que subimos a nuestro perfil y, así, una simple foto subida a la red social, descontextualizada, puede convertirse en fenómeno viral, *"que llegue a un número ingente de personas y que les provoque daños considerables a los sujetos afectados"*[57]. Uno de los riesgos importantes de las redes sociales, particularmente Facebook por su diseño y arquitectura, es el de la descontextualización de la información. *"Facebook tiene un diseño completamente distinto al del mundo físico, y sus propiedades arquitectónicas, temporales e interpersonales tienen el potencial de generar una asimetría entre los sentimientos de los usuarios y el modo en que se propaga la información"*[58]. Los datos son utilizados en contextos distintos para el cual se emitieron, *"en los espacios on-line que constituyen las redes sociales se rompen estas reglas contextuales, y lo que era dicho para un grupo cerrado de amigos, queda a disposición de la comunidad entera"*[59].

Por otra parte, estos servicios crean una falsa ilusión de que se trata de un servicio gratuito, cuando realmente éstos servicios se financian en muchos casos a través de la utilización secundaria de los datos personales, por ejemplo comercializándolos con fines de marketing personalizado. Tanto la información obtenida a través de las redes sociales, como por los buscadores *"es susceptible de ser utilizada para ofrecer publicidad basada en personas e intereses de una manera muy efectiva"*[60]. De hecho, las redes sociales se financian, sobre todo, a través del envío de publicidad personalizada, a través de la realización de sondeos de opinión entre los usuarios de la red social o a través de la explotación comercial de los contenidos protegidos por la propiedad intelectual, que los usuarios suben a la red social[61]. Debe tenerse en cuenta que una cuenta en una red social *"no es propiedad del usuario, es un espacio puesto a su disposición gratuitamente, a cambio de su disponibilidad a ser seccionado en*

[57] P. ESCRIBANO TORTAJADA, "Algunas cuestiones sobre la problemática jurídica del derecho a la intimidad, al honor y a la propia imagen en Internet y en las redes sociales", en A. FAYOS GARDÓ, *Los derechos a la intimidad y a la privacidad en el Siglo XXI*, Dykinson, Madrid, 2015, p. 71.

[58] F. DUMORTIER, "Facebook y los riesgos de la 'descontextualización' de la información", *Revista de Internet, Derecho y Política,* num. 9, 2009, p. 28.

[59] M.VILASAU SOLANA, *"Privacidad, redes sociales y el factor humano",* en A. RALLO LOMBARTE y R. MARTÍNEZ MARTÍNEZ (coord.), *Derecho y redes sociales*, cit., p. 61.

[60] A. SUÁREZ SÁNCHEZ-OCAÑA, *Desnudando a Google,* cit., p. 252.

[61] J-P. MOINY, "Facebook y la Directiva 95/46: algunas reflexiones", en Mª. R. LLÁCER MATACÁS, *Protección de datos personales en la Sociedad de la Información y la vigilancia*, cit., p. 179.

partes comercialmente interesantes"[62] y, como señala Zigmunt Bauman, en este ámbito, la socialización sigue las pautas del marketing y las herramientas electrónicas de la socialización digital *"están hechas a la medida de las técnicas de marketing"*[63].

Nuestra actividad en la red va a ser utilizada para obtener información sobre nosotros y sobre terceros. A través de la interacción en la redes sociales de terceros relacionados con una persona determinada se puede obtener, por ejemplo, información sobre su orientación sexual. Una red social puede inferir este tipo de información de usuarios, que no la han revelado, a través de las conexiones e interacciones con los demás usuarios que si han hecho pública su orientación sexual; pero, incluso en el caso de los denominados «perfiles en la sombra», es decir, los relativos a personas que no tienen cuenta en una red social, es posible inferir información privada sobre sus preferencias sexuales por lo que, no tener una cuenta en una red social, no garantiza un mayor nivel de privacidad, siempre y cuando uno tenga bastantes amigos que ya están en ella[64]. De esta forma, el nivel de privacidad de un individuo no va depender sólo de su comportamiento en línea, sino del aquellos otros con los que esté interconectado. Desde el momento en que los usuarios comparten su lista de contactos, aunque estos no estén en la red social, es posible colegir información privada sobre ellos y *"dado el hecho de que esta dependencia está presente bajo la interacción social generalizada, debemos considerar la privacidad como un concepto colectivo, donde las políticas de privacidad individuales no son suficientes para controlar la información privada"*[65]. Es decir, cuando un usuario sube información propia y de terceros a una red social está generando riesgos no sólo para su vida privada sino también directamente para aquellos cuyos datos sube, con o sin su consentimiento, e, indirectamente, para todos sus contactos en la medida en que se pueden inferir informaciones sobre ellos, incluso sensibles, a través de correlaciones.

---

[62] IPPOLITA, *En el acuario de Facebook. El irresistible ascenso del anarco-capitalismo*, cit., p. 64.

[63] Z. BAUMAN, *Vida de consumo,* trad. de Mirta Rosenberg y Jaime Arrambide, Fondo de Cultura Económica, Madrid, 2007, p. 157.

[64] E. SARIGOL, D. GARCÍA y F. SCHWEITZER, "Online Privacy as a Collective Phenomenon", *Proceedings of the second edition of the ACM conference on Online social networks*, ACM, octubre de 2014, p. 105. Puede consultarse en: *http://arxiv.org/pdf/1409.6197.pdf.*

[65] Ibídem.

2. PREDICCIONES Y CORRELACIONES BASADAS EN GRANDES CANTIDADES DE INFORMACIÓN PERSONAL: EL PANÓPTICO DIGITAL

Tradicionalmente se ha acudido, por su fuerza ilustrativa, para explicar el fenómeno de la vigilancia en la sociedad actual al modelo panóptico[66], inspirado en aquel modelo arquitectónico carcelario diseñado por Jeremy Bentham a finales del siglo XVIII con el objetivo de que el vigilante pudiera observar a todos los prisioneros, que se encuentran recluidos en celdas individuales, sin que estos sepan si son observados. Cada recluso se encuentra *"perfectamente individualizado y constantemente visible"*, con el fin de *"inducir en el detenido un estado consciente y permanente de visibilidad que garantiza el funcionamiento automático del poder"*[67]. En el mundo contemporáneo en el que las posibilidades de vigilancia de nuestras acciones cotidianas, online y of line, por ejemplo a través de las miles de cámaras de videovigilancia instaladas en tantos lugares de nuestras ciudades, carreteras y autopistas, son tan reales, el modelo panóptico resulta muy esclarecedor. En la sociedad digital, nos recuerda Bauman, "*los refugios tienen paredes permeables, perforadas por todas partes por infinidad de cables y atravesadas fácilmente por ubicuas emisiones de ondas*"[68].

Es un hecho que la tendencia a incrementar los sistemas de información y vigilancia para garantizar la seguridad es creciente, ocurre a ambos lados del atlántico, y *"la frecuencia con que los Estados procuran acceder tanto al contenido de las comunicaciones como a los metadatos de las comunicaciones aumenta drásticamente cada año, sin controles adecuados"*[69]. Se sitúa a la ciudadanía

---

[66] Vid. O. H. GANDY, *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, CO, Westview Press, 1993.

Asimismo, C. NORRIS, "From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control", en D. LYON (ed.): *Surveillance as Social Sorting*, Routledge, Londres y Nueva York, 2005 o J. REIMAN, "Driving to the panopticon: a philosophical exploration of the risks to privacy posed by higway technology of the future", en E. BARENDT (ed.): *Privacy*, Dartmouth Publishing Company, Aldershot, 2001.

También: Z. BAUMAN y D. LYON, *Vigilancia líquida,* traducción de Alicia Capel Tatjer, Paidós, Barcelona, 2013, p. 61 y ss.

Igualmente, H. BYUNG-CHUL, *La sociedad de la transparencia*, cit., p. 87 y ss.

[67] M. FOUCAULT, *Vigilar y castigar,* traducción de Aurelio Garzón del Camino, Siglo XXI Editores, Buenos Aires, 2002, p.185.

[68] Z. BAUMAN, *Modernidad líquida,* traducción de Mirta Rosenberg, Fondo de Cultura Económica, Buenos Aires, 2013, p. 165.

[69] V. DOMINGO PRIETO, "De la defensa del derecho fundamental a la privacidad a la vigilancia masiva", en E. R. JORDÀ CAPITÁN y V. DE PRIEGO FERNÁNDEZ, *La*

en la falsa tesitura de elegir entre seguridad y libertad, cuando en una sociedad democrática debe encontrarse el equilibrio entre ambos intereses[70]. El modelo panóptico sirve tanto para reflejar la vigilancia realizada por los Estados por razones de seguridad, que clasifica a los individuos en función de su peligrosidad, como para evidenciar las prácticas del marketing comportamental que clasifica a los individuos en función de su valor económico o su potencial como posibles compradores[71] o como consumidores fallidos[72]. Debe señalarse que este modelo ha recibido numerosas críticas al considerarse superado por otros modelos explicativos más ajustados a la realidad presente, en la que la vigilancia electrónica que se ha movido más allá de los confines de una sola cárcel y a menudo nos rodea[73]. Sin embargo, el panóptico se niega a desaparecer por su fuerza explicativa y aparece habitualmente en los discursos sobre vigilancia[74], si bien han surgido nuevos modelos que suponen su reformulación para adaptarse a la nueva realidad de la vigilan-

protección y la seguridad de la persona en Internet. Aspectos sociales y jurídicos, Editorial Reus, Zaragoza, 2014.

[70] Si bien excede el objeto de este trabajo el análisis de la vigilancia masiva de las comunicaciones de sus ciudadanos y de ciudadanos de terceros países realizada por Estados democráticos, a modo de ejemplo de tales prácticas pueden citarse las conclusiones del Parlamento Europeo recogidas en su Resolución de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior (2013/2188(INI)). El Parlamento Europeo consideró acreditada *"la existencia de sistemas tecnológicamente muy avanzados, complejos y de amplio alcance diseñados por los servicios de inteligencia de los Estados Unidos y de algunos Estados miembros para recopilar, almacenar y analizar datos de comunicaciones, incluidos datos de contenido y datos y metadatos de localización de todos los ciudadanos en todo el mundo a una escala sin precedentes y de una manera indiscriminada y no basada en sospechas"*. En concreto, en la Resolución se citan entre otros sistemas de interceptación de las comunicaciones *"los programas de inteligencia de la Agencia Nacional de Seguridad estadounidense que permiten la vigilancia masiva de ciudadanos de la UE mediante un acceso directo a los servidores centrales de empresas estadounidenses líderes en Internet (programa PRISM), el análisis de contenido y metadatos (programa Xkeyscore), la elusión del cifrado en línea (BULLRUN), el acceso a redes informáticas y telefónicas y el acceso a los datos de localización, así como algunos sistemas de la agencia de inteligencia británica GCHQ, como por ejemplo la actividad preliminar de vigilancia (programa Tempora), el programa de descifrado (Edgehill), los ataques selectivos con intermediarios contra sistemas de información (programas Quantumtheory y Foxacid) y la recopilación y retención de 200 millones de mensajes de texto al día (programa Dishfire)."*

[71] Vid. O. H. GANDY, *The Panoptic Sort: A Political Economy of Personal Information*, cit.

[72] Z. BAUMAN, *Vida de consumo,* cit., p. 82.

[73] B. W. SCHERMER, *Surveillance and Privacy in the Ubiquitous Network Society*, cit.

[74] D. LYON, *The search for surveillance theories*, cit., p. 4.

cia tecnológica. Así por ejemplo, el "banóptico", que haría referencia a cómo las tecnologías de la elaboración de perfiles a través de la reconstrucción de las trayectorias individuales o sociales, marcan territorios o fronteras entre las poblaciones en riesgo, para analizar y decidir quién es peligroso y por lo tanto quién ha de ser objeto de una vigilancia estricta[75] o el "superpanóptico", que se centraría en como en la sociedad de la computación ubicua, que se encuentra por todas partes, habrá cada vez más información disponible y posibilitará la vigilancia en tiempo real de los individuos.

En un futuro cercano, el mundo digital y el mundo físico estarán estrechamente entrelazados y los operadores de vigilancia tendrán incluso la capacidad de desencadenar eventos y acciones desde la distancia y, en consecuencia, la vigilancia cambiará de una "arquitectura de la observación" a una «arquitectura de control», lo que tendrá un enorme impacto negativo en la autonomía de los individuos y de los grupos en los que estos se integran[76]. En el mundo de la vigilancia ubicua se almacena información sobre determinados individuos por sus propias características o incluso por sus relación con otros que se consideran peligrosos, con independencia de que se trate de menores de edad y de los riesgos de exclusión, discriminación y estigmatización que conlleva[77]. En el Estado vigilante se está operando un cambio en el modelo de las políticas públicas de seguridad y lucha contra la delincuencia pasando de un modelo basado en la sanción de las conductas infractoras de las normas jurídicas a un modelo basado en *"categorías sospechosas"*[78] en el que se tiende *"al control de riesgos sociales a través de «adelantamiento de la punibilidad», un modelo en el que la perspectiva del ordenamiento jurídico-penal es prospectiva, es decir, cuyo punto de referencia es, cada vez más, el hecho futuro"*[79].

---

[75] D. BIGO, *"Security, exception, ban and surveillance,* cit., p. 46 y ss.

[76] B. W. SCHERMER, *Surveillance and Privacy in the Ubiquitous Network Society*, cit., p. 67 y 68.

[77] Vid. House of Lords: *Second Report, Surveillance: Citizens and the State:*

"Moves are already underway to try to identify children who may grow up into one of the 20% of adults who are believed to commit 80% of the crime. This involves analysing circumstantial risk factors such as family members' criminal records. This runs the real risk that children are stigmatised from an early age and however well behaved they may be are treated with suspicion."

El informe puede consultarse en:

http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm

[78] Vid. Z. BAUMAN, Miedo líquido. La sociedad contemporánea y sus temores, trad. de Albino Santos Mosquera, Paidós, Barcelona, 2007, p. 159.

[79] A. NIETO MARTÍN y M. MAROTO CALATAYUD, "Redes sociales en Internet y 'data mining' en la prospección en investigación de comportamientos delictivos", en A.

Como consecuencia del desarrollo tecnológico, es previsible que, cada vez más, la vida diaria estará bajo vigilancia constante: los seres humanos estarán rodeados, inmersos en la informática y las tecnologías en red desde el amanecer hasta el atardecer y en cada lugar concebible[80]. A esta realidad contribuirán activamente también los «moradores del panóptico digital» a través de la hipercomunicación. A diferencia del panóptico de Bentham que buscaba el control a través del aislamiento, señala Byung-Chul, *"la peculiaridad del panóptico digital está sobre todo en que sus moradores mismos colaboran de manera activa en su construcción y en su conservación, en cuanto se exhiben ellos mismos y se desnudan"*[81].

Esta situación convierte en insuficientes e inapropiadas las categorías artificiales de clasificación de las informaciones (comunicación, metadato, datos del proveedor, datos en tránsito, etc.) para medir *"el grado de intromisión que la vigilancia de las comunicaciones realiza en la vida privada y las relaciones de las personas"*[82]. Los datos obtenidos a través de los sensores, las aplicaciones y los servicios tecnológicos pueden, por sí solos o analizados en conjunto, proyectar perfiles sobre personas directamente o a través de correlaciones cuando se buscan patrones utilizando la tecnología de minería de datos. Los actuales niveles y sistemas de vigilancia en los que las tecnologías digitales y los datos personales ocupan un lugar fundamental en orden a la clasificación de las personas, producen peligros profundos para la democracia y las posibilidades de participación democrática, la crítica o disensión ética y los movimientos sociales alternativos[83].

Ya no resulta novedoso señalar la situación de *"erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías"*[84]. Es indudable que durante las últimas décadas se ha ido haciendo patente que una de las mayores amenazas a la dignidad, a la libertad y a los derechos de los ciudadanos provenía de la capacidad de acumular

---

RALLO LOMBARTE y MARTÍNEZ R. MARTÍNEZ (coord.), *Derecho y redes sociales*, Civitas, Madrid, 2010, p. 210.

[80] D. LYON, *Surveillance Studies. An overwiew*, Polity Press, Malden, 2014, p. 1.

[81] H. BYUNG-CHUL, *La sociedad de la transparencia*, cit., p. 89.

[82] V. DOMINGO PRIETO, *De la defensa del derecho fundamental a la privacidad a la vigilancia masiva*, cit., p. 39.

[83] Vid. D. LYON, *Surveillance Studies. An overwiew*, cit., p. 5 y ss.

[84] A. E. PÉREZ LUÑO, "Intimidad y protección de datos personales: del Habeas Corpus al Habeas Data" en L. GARCÍA SAN MIGUEL, Estudios sobre el derecho a la intimidad, Tecnos, Madrid, 1992, p. 37.

informaciones personales. Datos que suministramos para finalidades concretas, posteriormente son cedidos y desviados para otras diferentes sin que se nos proporcione ningún tipo de información acerca de su destino o, en muchos casos, sin que siquiera, seamos conscientes de ello. Pero, en la era de los datos masivos, a las posibilidades de almacenamiento y reutilización de la información personal hay que añadir la utilización de potentes herramientas de análisis, provocando *"lo que gráficamente se ha denominado como la muerte de la amnesia"*[85]. La participación en una manifestación, en un «botellón» callejero, un comentario desafortunado en un red social o cualquier comportamiento *online,* puede quedar registrado de por vida, con el peligro de que entidades privadas o el Estado pueda *"hacer resucitar el pasado de cualquier ciudadano en cualquier momento con todo lujo de detalles"*[86].

En la sociedad digital, obsesionada con la diferenciación, la clasificación y en la que todo se archiva, el control se ejerce por parte del mercado a través de la tentación y la seducción mediante técnicas en las que *"la voluntad, ni siquiera entusiasta, y la cooperación de los manipulados es el principal recurso empleado por los sistemas sinópticos de marketing"*[87]. En el ámbito del Estado, las TIC dotan cada vez de mayor sentido a *"la sociedad de control que se sostiene mediante el discurso de la seguridad y la prevención, de garantizar la misma vida que controla"*[88].

Una de las cuestiones centrales en el tratamiento de la información sobre personas es la de la determinación de sus fines. El marketing y la prevención y la persecución de los delitos son dos de esos fines, pero el fenómeno es mucho más amplio. Personas ajenas a nuestro entorno toman determinadas decisiones que nos afectan en base a datos e informaciones personales que nosotros no hemos suministrado o lo hemos hecho para alguna finalidad concreta, o que simplemente considerábamos olvidadas o secretas. En el ámbito financiero o en el de los seguros se utilizan perfiles de riesgo de forma habitual. Además el Big Data va a ampliar estas posibilidades a través del uso de correlaciones utilizando, por ejemplo, *"informes crediticios y datos de marketing de consumo como aproximación a los análisis de sangre y de orina para*

---

[85] A. NIETO MARTÍN y M. MAROTO CALATAYUD, *Redes sociales en Internet y 'data mining' en la prospección en investigación de comportamientos delictivos*, cit., 212.

[86] Ibídem.

[87] Z. BAUMAN y D. LYON, Vigilancia líquida, cit., p. 140.

[88] J. M. CORTÉS, *La ciudad cautiva. Control y vigilancia en el espacio urbano,* Akal, Madrid, 2010, p. 32.

determinados solicitantes"[89] de sus productos o servicios e identificar a aquellos que tengan un mayor riesgo de padecer hipertensión, depresión o diabetes. Obviamente, la finalidad de ese procesamiento de información personal es determinar la prima del seguro o, incluso, excluir a determinados grupos de personas del acceso a estos servicios. Debemos ser conscientes de que el proceso de mercantilización de los datos personales aparenta ser irreversible en la sociedad digital. Por la propias reglas del libre mercado, *"los datos pasan de ser elementos constitutivos de la esfera personal, susceptibles de circular en el mercado a través del libre consentimiento, a ser una mercancía más de un proceso de producción, intercambio y consumo"*[90].

Como consecuencia de este ensanchamiento de la posibilidad de indagación sobre la vida de las personas se producirá una mayor influencia y presión sobre las propias decisiones. Así por ejemplo, una de los efectos de la publicidad comportamental o dirigida es que, por una parte, puede influir en los deseos de nuevas maneras, pero por otra, la publicidad basada en perfiles también puede influir en los comportamientos reales de ciertos grupos sociales que, como los individuos, son alentados por retroalimentación para ajustarse a los patrones esperados[91]. En la sociedad de consumo, sociedad sinóptica de adictos compradores/espectadores, *"la obediencia al estándar (…) tiende a lograse por medio de la seducción, no de la coerción… y aparece bajo el disfraz de la libre voluntad, en vez de revelarse como una fuerza externa"*[92]. Es un algoritmo quien nos dirá que es lo que deseamos realmente, corrige nuestras búsquedas en Google, nos dice cuáles son nuestros amigos potenciales en las redes sociales, nos indica cuáles son las películas, los libros o la música que se adaptan mejor a nuestros gustos o nos indica *"qué personas podríamos querer seguir en Twitter"*[93]. Obviamente, cuanto más información se recabe sobre una persona y más preciso sea su perfil, más fácil será orientar, dirigir, tentar y seducir. Quienes controlan la información saben más de algunas personas que ellas mismas[94], pero, además, *"la exploración de los datos hace visibles mo-*

[89] V. MAYER-SCHÖNBERGER y K. CUKIER, *Big data. La revolución de los datos masivos,* cit., p. 76.

[90] A. SÁNCHEZ, H. SILVEIRA y M. NAVARRO, *Tecnología, intimidad y sociedad democrática*, cit., p. 41.

[91] D. LYON, *Surveillance Studies. An overview*, cit., p. 101.

[92] Z. BAUMAN, *Modernidad líquida*, cit., p. 92.

[93] IPPOLITA, *En el acuario de Facebook. El irresistible ascenso del anarco-capitalismo*, cit., p. 105.

[94] Un ejemplo de este tipo de prácticas son los sistemas de seguimiento de compras para asociar recomendaciones y dirigir compras futuras.

delos colectivos de comportamiento de los que ni siquiera somos conscientes como individuos"[95], lo que también contribuirá a que los resultados de análisis del comportamiento puedan ser más precisos y más útiles para diversas finalidades. Por ello, nos encontramos ante el riesgo de que se produzca *"el más implacable fenómeno de control y manipulación social que pueda imaginarse"*[96]. Por estas razones, la protección de la vida privada sigue siendo un derecho ineludible para garantizar la individualidad y la libertad de los seres humanos[97].

Las peculiaridades sociales, económicas, tecnológicas y políticas de nuestra civilización propician que la recogida y acumulación de información personal muchas veces incluso de forma indiscriminada, se dispare hasta la exageración. El actual desarrollo de las tecnologías de la información y la comunicación posibilitan la recogida y utilización de información sobre las personas de manera ilimitada, el capitalismo imperante propicia no sólo la crisis de los derechos sociales, cada vez más limitados, sino también graves mermas en las libertades individuales clásicas como el derecho a la intimidad a cambio de mayores rendimientos económicos e incrementos en la rentabilidad a cualquier precio. Por otra parte, nuestras sociedades desarrolladas se han acostumbrado a conocer la vida privada de todo tipo de personas, públicas o anónimas, que están dispuestas a vender la exclusiva de su vida personal o familiar o incluso a vivir en auténticas cajas de cristal a cambio de una notoriedad efímera y patética. Fenómenos como los *reality shows*, las redes sociales o los blogs, entre otros, están contribuyendo de manera decisiva a un nivel de exposición pública de la vida privada sin precedentes. En la época de Facebook y Photoshop el rostro humano se transforma en *"una faz que se disuelve por entero en su valor de exposición (y) en la sociedad expuesta, cada sujeto es su propio objeto de publicidad"*[98]. En la «modernidad líquida» se ha producido la colonización del espacio público por temas que antes considerábamos privados e inadecuados para ser expuestos en público. Los problemas privados pueden discutirse en público y no sólo se está renegociando la frontera entre los privado y lo público, sino que *"está en juego una redefinición de la esfera pública como plataforma dónde se ponen en escena los dramas privados a la vista del público"*[99].

---

[95] H. BYUNG-CHUL, *En el enjambre,* cit., p. 109.

[96] A. E. PÉREZ LUÑO, *La contaminación de las libertades en la sociedad informatizada y las funciones del Defensor del Pueblo, Anuario de derechos humanos*, num. 4, 1986-1987, p. 269.

[97] W. A. PARENT, "Privacy, Morality and Law", en E. BARENDT (ed.), *Privacy*, Dartmouth Publishing Company, Aldershot, 2001, p. 112.

[98] H. BYUNG-CHUL, *La sociedad de la transparencia,* cit., pp. 27 y 29.

[99] Z. BAUMAN, *Modernidad líquida,* cit., p. 75.

Todo ello ha contribuido a fomentar una ideología de transparencia radical[100] en la que nos sentimos con derecho a conocer, observar y juzgar las alegrías y miserias de los demás, incluso las de aquellos que desean mantenerlas fuera de nuestro alcance y juzgamos que aquél que no está dispuesto a mostrarse desnudo ante nuestra mirada curiosa y ociosa es por que tiene algo que ocultar. La transparencia es el imperativo de la sociedad digital: *"todo tiene que estar ahí abierto como información, de manera accesible a cualquiera. La transparencia es la esencia de la información. Es la manera de proceder del medio digital"*[101].

3. LA REGULACIÓN DE LA ADOPCIÓN DE DECISIONES AUTOMATIZADAS Y DE LA ELABORACIÓN DE PERFILES EN EL NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

Ante los retos que plantean las tecnologías y las prácticas descritas, la normativa de protección de datos personales aprobada en el siglo XX sólo puede ofrecer unos mecanismos de protección parciales e insuficientes. Para hacer frente a los actuales retos en esta materia de protección de datos personales y tras un largo proceso, que se inició en 2010 por la Comisión Europea[102], se aprobó el nuevo Reglamento General de protección de Datos[103]. En el Reglamento Europeo, como no podía ser de otra forma, se regulan la elaboración de perfiles y el derecho a no ser objeto de decisiones basadas únicamente en tratamiento automatizados. Me centraré exclusivamente en los aspectos que afectan más directamente a esta cuestión, ya que

---

[100] IPPOLITA, *En el acuario de Facebook. El irresistible ascenso del anarco-capitalismo*, cit., p. 51 y ss.

[101] H. BYUNG-CHUL, *En el enjambre*, cit., p. 64 y 65.

[102] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. Un enfoque global de la protección de los datos personales en la Unión Europea. Bruselas, 4 de noviembre de 2010.

Asimismo vid. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI. Bruselas, 15 de enero de 2012.

[103] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

es imposible en un trabajo de estas características hacer un estudio completo y sistemático de todos los preceptos que tendrían incidencia sobre ella.

Podemos considerar como antecedentes de esta regulación, además del artículo 15 de la Directiva 95/46/CE al que me referiré más adelante, la Recomendación (2010)13 sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles del Comité de Ministros del Consejo de Europa. En la Recomendación se señala que en la era del Big Data, cuando el desarrollo actual de las TIC permite *"la recopilación y el tratamiento de datos a gran escala, incluidos datos de carácter personal, en los sectores tanto público como privado"*, los datos son tratados *"por programas de cálculo, de comparación y de correlación estadística, con el objetivo de crear perfiles que puedan utilizarse de diversas formas para diferentes fines y usos"*. Si bien es cierto, que en determinados ámbitos *"la creación de perfiles puede obrar en el interés legítimo tanto de la persona que la utiliza como de aquella a la que se aplica, por ejemplo, al conducir a una mejor segmentación de los mercados, permitir un análisis de los riesgos y del fraude, o adaptar la oferta a la demanda mediante la prestación de unos mejores servicios"*, y, por lo tanto, tener ventajas para los usuarios, la economía y la sociedad en general, la Recomendación identifica los posibles problemas que esta tecnología implica para los derechos y la dignidad de las personas.

En primer lugar, a través de la conexión de un gran número de datos individuales, incluso anónimos, la técnica de creación de perfiles puede conducir a incluir a las personas en categorías predeterminadas sin que tengan conocimiento de ello. Esta falta de transparencia en los procesos de creación de perfiles y en su posterior aplicación, así como *"la falta de precisión que puede derivarse de la aplicación automática de reglas de inferencia preestablecidas, pueden suponer graves amenazas para los derechos y libertades de las personas"*. Por otra parte, la atribución de perfiles a una persona determinada puede generar nuevos datos personales, que no son los que el interesado había proporcionado. En consecuencia podría verse afectado el control de la propia identidad de la persona interesada, se le podría privar de manera arbitraria del acceso a ciertos bienes o servicios, violando como consecuencia el principio de no discriminación. Los efectos de estas operaciones serán especialmente graves cuando se realicen correlaciones utilizando datos sensibles, lo que supondrá *"exponer a las personas a riesgos particularmente elevados de discriminación y de atentados contra sus derechos personales y su dignidad"*. También serán especialmente graves estas prácticas cuando la creación de perfiles se refiera

a niños, ya que podrían tener graves consecuencias para ellos a lo largo de toda su vida.

La Recomendación fija una serie de principios para garantizar los derechos fundamentales ante tales prácticas que van desde la adopción del principio de privacidad desde el diseño hasta garantizar la neutralidad[104] y la transparencia de estos procedimientos.

También resulta relevante recordar los principios expresados en Resolución de Varsovia sobre *profiling* de la de la XXXV Conferencia Internacional de Autoridades de Protección de datos y Privacidad[105]:

- Debe determinarse claramente en cada caso concreto la necesidad de *profiling* y establecerse garantías adecuadas antes del inicio de esa operación.
- Deben respetarse las normas sobre calidad de los datos, en especial, los principios de pertinencia y finalidad, exactitud y veracidad, en

[104] El principio de neutralidad de la tecnología surge para contrarrestar el desequilibrio existente entre el usuario de los productos tecnológicos, que no tiene conocimientos específicos, y los responsables de la tecnología, que predisponen los sistemas de tratamiento de datos personales. Si la tecnología no es neutra, es decir, condiciona la autonomía de su destinatario e impone *"formas onerosas de ejercer los derechos (…), se convierte en un factor de dominación"* (En M. R. LLÁCER MATACÁS, *La autodeterminación informativa en la sociedad de la vigilancia: Ubiquitous Computing,* cit., p. 89). El principio de neutralidad está íntimamente conectado con los principios de privacidad desde el diseño y por defecto, ya que lo que se requiere es una mayor responsabilidad en la planificación y el diseño tecnológico para garantizar el derecho a la vida privada de los usuarios de esa tecnología. A través de este principio se trataría de contrarrestar la técnica contraria, tan común en muchos servicios de Internet que consiste en *"deshabilitar al máximo la privacidad de las aplicaciones por sus titulares"* (En A. TOURIÑO, *El derecho al olvido y a la intimidad en Internet,* Catarata, Madrid, 2014, p. 23). El principio de neutralidad supone, por lo tanto, incluir dentro de la previsiones técnicas una más: la consideración de que esa tecnología debe ser respetuosa con los derechos humanos. El principio de neutralidad tecnológica está muy relacionado con el principio de privacidad desde el diseño, que aparece en la década de los noventa promovido por Ann Cavoukian, Comisionada de Información y Privacidad de Ontario y se extendería a una «trilogía» de aplicaciones que englobarían los sistemas de tecnologías de la información, las prácticas de negocio responsable y el diseño físico e infraestructura en red (Vid. A. CAVOUKIAN, *Privacy by Design. The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*, Information and Privacy Commissioner of Ontario, Canadá, 2010.Puede consultarse en: *https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.).*

[105] Con anterioridad manifestados en la Declaración de Uruguay sobre de 2012 sobre *Profiling* la XXXV Conferencia Internacional de Autoridades de Protección de datos y Privacidad.

consonancia con los principios de privacidad basada en el diseño y el volumen de datos recogidos.

- Es necesario validar continuamente los perfiles y los algoritmos subyacentes, con el fin de permitir la mejora de los resultados y la reducción de los falsos positivos o falsos negativos.
- Debe proporcionarse a la sociedad una información clara y transparente sobre este tipo de operaciones, "*incluyendo el modo en el que los perfiles son ensamblados y los fines para los que son utilizados, con el fin de asegurar que los individuos son capaces de mantener el control sobre sus propios datos personales en la mayor y más adecuada medida posible*".
- Deben garantizarse los derechos de los interesados a la información, acceso y rectificación y, en particular, "*respecto a las decisiones que tengan significativos efectos legales en las personas o que afecten a sus beneficios o a su estatus, así como que se provea de intervención humana cuando resulte adecuado, especialmente en la medida en la que el poder predictivo del profiling se incrementa debido a algoritmos cada vez más eficaces*".
- Todas las operaciones de elaboración de perfiles deben estar sujetas a una supervisión adecuada.

En su redacción definitiva, el artículo 22 del Reglamento garantiza el derecho del interesado *a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles*[106]*, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*, teniendo en cuenta los principios anteriores. Su redacción es bastante semejante al artículo 15 de la Directiva 46/95/CE que reconoce el derecho de las personas a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, basada exclusivamente en un tratamiento automatizado de datos destinados a evaluar determinados aspectos de su personalidad. También como en el caso de la Directiva, no estamos ante un derecho absoluto, estableciéndose una serie de excepciones. Este derecho no se aplicará cuando la decisión sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento,

[106] En el Considerando 71 del Reglamento se ejemplifican varios tipos de perfiles posibles que consistirían en "*cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar*".

cuando esté autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o se base en el consentimiento explícito del interesado. También es este caso la regulación del Reglamento coincide con la Directiva, que permitía que una persona pudiera verse sometida a una decisión automatizada cuando se adoptase en el marco de un contrato o cuando una ley lo autorizase estableciendo medidas que garantizasen el interés legítimo del interesado.

En dichos casos, corresponderá al responsable del tratamiento adoptar las medidas *adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión*. Por lo tanto, al igual que en la Directiva 95/46/CE no se prohíbe la elaboración de perfiles sino que limitan los casos en los que una persona podrá ser objeto de una decisión automatizada que le afecte significativamente y se garantiza el derecho a obtener participación humana y a impugnar la decisión.

Se establece, además, una limitación en razón de la naturaleza de los datos personales prohibiéndose la adopción de decisiones automatizadas basadas en datos sensibles (origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales) salvo que el interesado de su consentimiento explícito y esta posibilidad no esté prohibida por el Derecho de la Unión o de los Estados miembros o cuando el tratamiento sea necesario por razones de un interés público esencial con base en el Derecho de la Unión o de los Estados miembros en los términos del art. 9.2 g) del Reglamento y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

En relación con las técnicas de elaboración de perfiles para la adopción de decisiones automatizadas resulta de vital importancia para garantizar los derechos fundamentales de las personas el respeto escrupuloso de los principios de calidad de los datos y en especial del principio de transparencia.

En el Reglamento las referencias al principio de transparencia son constantes, al menos en su parte expositiva. Son muchos los Considerando que recogen la obligación de que se facilite al interesado de forma sencilla, fácilmente accesible y en un lenguaje claro y sencillo, toda la información rele-

vante para él en el proceso de tratamiento de sus datos. En concreto deberá facilitársele información sobre la identidad del responsable del tratamiento y los fines del mismo, sobre los riesgos, las reglas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento (Considerando 39).

El Considerando 58 determina que toda información dirigida al público o al interesado sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro y, además, cuando proceda, se visualice, estableciéndose previsiones para que la información pueda facilitarse en formato electrónico, por ejemplo, cuando esté dirigida al público, mediante un sitio web. En el Reglamento esta obligación es especialmente pertinente *"en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea"* y además, si la información se dirige a niños, deberá adaptarse el leguaje para que les sea fácilmente comprensible.

Específicamente, para garantizar un tratamiento leal y transparente respecto del interesado en el ámbito de la elaboración de perfiles, en el Considerando 71 se establece la necesidad de que el responsable del tratamiento utilice procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicando medidas técnicas y organizativas apropiadas para garantizar *"que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto"*.

El principio de transparencia está íntimamente ligado al derecho a recibir una información completa, clara y sencilla relativa a todos los aspectos relevantes de un tratamiento de datos personales y a las posibles consecuencias que se podrían derivar de ese tratamiento. Parece evidente que de lo primero que habría que informar es de la existencia de esos tratamientos sobre todo en el ámbito de Internet en el que nuestros datos son recopilados por multitud de proveedores de servicios sin que seamos conscientes de ello. Cuanto más sensible sean los datos o el conjunto de operaciones a los que se les someta en el ámbito de la elaboración de perfiles para tomar decisiones

sobre las personas, más exigente debiera ser el cumplimiento del principio de transparencia. La exigencia de transparencia debe ser configurada como *"un derecho prestacional que requiere una actuación positiva por parte de las autoridades públicas"*[107] y se conecta con el establecimiento de un contenido pormenorizado del derecho de información y de las correlativas obligaciones informadoras del responsable del tratamiento.

El principio de transparencia se encuentra incluido entre los principios relativos al tratamiento regulados por el artículo 5 del Reglamento y se desarrolla en el artículo 12, que obliga al responsable del tratamiento a adoptar las medidas oportunas para facilitar al interesado toda información relevante relativa al tratamiento de sus datos personales incluida la existencia de decisiones automatizas y la elaboración de perfiles así como *información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de dicho tratamiento para el interesado* (artículo 13). El principio de transparencia obliga al responsable del tratamiento a garantizar que se le informa aún cuando los datos no se hayan obtenido directamente de interesado en los términos previstos en el artículo 14 y a garantizar el derecho de acceso, así como cualquier comunicación al interesado que se refiera al tratamiento de sus datos en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño.

El cumplimiento de este principio es de la mayor importancia para garantizar uno de los derechos previstos en el artículo 22, la impugnación de la decisión automatizada basada en un perfil, cuando está este permitida. La impugnación de las decisiones fundamentadas exclusivamente en un tratamiento de datos personales, tratan de contrarrestar los efectos perjudiciales que pueden derivarse para un individuo en sus relaciones públicas o privadas, de la reconstrucción artificial de su perfil personal, en base al tratamiento de sus datos y en numerosas ocasiones simplemente en base a datos estadísticos relativos al grupo social al que pertenece, barrio en el que reside, etc. Por otra parte, debe tenerse en cuenta, además, que la conclusión a la que se llegue –el perfil informático obtenido– a través de dicho tratamiento puede no corresponderse con la realidad. Este derecho cobra una nueva y mayor

[107] Vid. B. TOMÁS MALLÉN, "Transparencia y protección de datos: nuevos desafíos para la garantía europea de los derechos fundamentales", en A. RALLO LOMBARTE y R. GARCÍA MAHAMUT, *Hacia un nuevo Derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015, p. 832 y ss.

relevancia en el mundo de los datos masivos, de la computación ubicua y del Internet de las cosas, ya que la adopción de decisiones sobre las personas en base a perfiles y correlaciones serán cada vez más frecuentes y las vías de obtención de los datos se multiplicarán.

4. CONSIDERACIONES FINALES

El procesamiento de la información sobre personas posibilita su clasificación social y la adopción de determinadas decisiones que le afectan. El uso del perfil informático podrá significar su discriminación en muchas de las actividades de la vida cotidiana. De hecho, el mayor de los riesgos en la omnipresente vigilancia que nos rodea no es para la erosión de la privacidad, sino para la igualdad, ya que las técnicas de clasificación y la elaboración de perfiles favorecen y confirman la formación de estereotipos sociales determinando, tanto la atribución de privilegios y derechos, como la exclusión social[108]. Ante este hecho nos encontraremos indefensos si desconocemos quién decide, en base a qué informaciones o cómo se establecen las diferentes categorías que servirán para el proceso de clasificación social.

La obtención del *perfil* supone establecer una correlación entre la posesión de determinadas características y comportamientos concretos. Es decir, implica encuadrar a una persona en un determinado grupo con particularidades determinadas, cuya utilización en la toma de decisiones, que afecten a los sujetos de tales operaciones, pueden suponer una valoración desfavorable de sus rasgos y características personales, lo que al final supondría su discriminación en el acceso a determinados bienes o servicios o la harían acreedora de una especial vigilancia y control al encajar en el perfil del posible delincuente o terrorista, del consumidor fallido, o del disidente de la ideología mayoritaria. Por otra parte, el uso de perfiles puede determinar incluso la información a la que vamos a tener acceso, limitando también nuestro derecho a recibir información veraz o siendo objeto de auténticas manipulaciones. A través de los distintos algoritmos utilizados por servicios como Facebook o Google, unos usuarios tienen acceso a un tipo de información y otros, en función de sus intereses o de su perfil ideológico[109], a otros contenidos diferentes y, en ocasiones,

[108] D. LYON, *Surveillance Studies. An overview*, cit., p. 184 y 185.

[109] Vid. E. BAKSHY, S. MESSING y L. A. ADAMIC, "Exposure to ideologically diverse news and opinion on Facebook", *Science,* vol. 348, num. 6239, 2015, p. 1130-1132. Puede consultarse en: *http://www.sciencemag.org/content/348/6239/1130.short.*

bajo la coartada del experimento sociológico, incluso se realiza sin tapujos una directa manipulación emocional de los usuarios[110].

A través de la elaboración del perfil se predice el comportamiento futuro y en función de ese posible comportamiento o reacción del individuo se adoptarán decisiones, favorables o desfavorables, pero potencialmente discriminatorias.

En el ámbito del mercado, el sistema banóptico de consumo basado en la construcción de perfiles tiene como consecuencia la "desmarketización" de los consumidores y en los demás sistemas banópticos que abundan en los espacios urbanos, puede tener como consecuencia que se impida *"el acceso a los servicios esenciales a las poblaciones proscritas conforme a sus perfiles personales"*[111], o en determinados casos que se valoricen *"algunos distritos y se demonicen otros"*[112].

El "perfilado", en el mundo de los datos escasos se basa en encontrar una asociación común, una regla general, que define a un grupo de personas a las que les es aplicable y se las somete a un escrutinio añadido. Por ejemplo, *"los individuos que presentan ciertas características sufren más registros en el aeropuerto"*[113]. Pero en el mundo de los datos masivos, los perfiles grupales serán sustituidos por predicciones mucho más individualizadas y personalizadas y *"las previsiones sobre individuos basadas en datos masivos pueden ser utilizadas en la práctica para castigar a la gente por sus propensiones y no por sus acciones"*[114], lo que niega el libre albedrío y la dignidad humana.

El establecimiento de perfiles afecta a las oportunidades vitales de las personas, que dependen de la categoría en la que las hayan situado. Esta realidad hace muy importante el principio de transparencia para poder cono-

---

[110] A lo largo de una semana durante el año 2012, Facebook experimentó con 689.000 ususarios sin su consentimiento para analizar su comportamiento alterando el algoritmo que selecciona las noticias que se ven de los amigos y, a través del tipo de noticias que mostraba a unos u a otros, positivas o negativas, para estudiar como influía en su estado de ánimo. Vid. A. KRAMER, D. I., GUILLORY, J. E. y J. T. HANCOCK, "Experimental evidence of massive-scale emotional contagion through social networks", *Proceedings of the National Academy of Sciences of Unites States of America,* vol. 11, num. 24, marzo de 2014.

[111] Z. BAUMAN y D. LYON, *Vigilancia líquida*, cit. p. 133 y 134.

[112] Ibídem.

[113] V. MAYER-SCHÖNBERGER y K. CUKIER, *Big data. La revolución de los datos masivos,* cit., p. 199.

[114] Ibídem, p. 210.

cer quién diseña esas categorías, quién decide sus significado y quién decide bajo qué circunstancias esas categorías serán decisivas[115].

El uso desviado de la tecnología de tratamiento de datos personales supone claros peligros para la libertad, para el derecho a nos ser discriminado y, asimismo, para la propia dignidad personal. El perfil informático instaura un determinismo incompatible con la autodeterminación, la presión del «juicio universal permanente»[116] puede producir mermas intolerables en la libertad individual; pues, que las decisiones que nos afecten se tomen en base a un precipitado automatizado de la personalidad supone, no solamente ser juzgado sin poder contradecir el resultado y sus consecuencias, sino también la posibilidad de ser discriminado y excluido. El ser humano pasa a ser mero objeto de información, dejando de ser un ser dotado de dignidad y sujeto de derechos fundamentales.

Por todo lo anterior, la protección de los datos personales en las nuestras sociedades debe perseguir, además de la genérica protección de la dignidad, la libertad y el disfrute de los derechos fundamentales de los ciudadanos, *"el equilibrio entre poderes y situaciones que es condición indispensable para el correcto funcionamiento de una comunidad democrática de ciudadanos libres e iguales"*[117] y, en la época de los datos masivos, deberemos sustraernos a la dictadura de los datos ya que corremos el riesgo de fetichizar, tanto la información, como el resultado de su análisis. Pues, manejados de forma responsable los datos masivos servirán para adoptar decisiones racionales; pero *"empleados equivocadamente, pueden convertirse en un instrumento de poder, que algunos pueden convertir en una fuente de represión, bien simplemente frustrando a consumidores y empleados, o bien –y es peor– perjudicando a los ciudadanos"*[118].

En el mundo del Big Data y de la computación ubicua se hace imprescindible garantizar que en los procesos de decisiones automatizadas sobre personas se extremen al máximo las garantías legales y se adopten rigurosamente los principios de transparencia y consentimiento del interesado, así

[115] D. LYON, *Surveillance Studies. An overview*, cit., p. 186.

[116] Vid. A. E. PÉREZ LUÑO, *Vittorio Frosini y los nuevos derechos de la sociedad tecnológica,* en Informatica e Diritto, vol. 1-2, Edizioni Scientifiche Italiane, 1992, p. 104.

[117] A. E. PÉREZ LUÑO, "Sobre el arte legislativo de birlibirloque. La LOPRODA y la tutela de la libertad informática en España", *Anuario de Filosofía del Derecho*, Tomo XVIII, 2001, p. 361.

[118] V. MAYER-SCHÖNBERGER y K. CUKIER, *Big data. La revolución de los datos masivos,* cit., p. 188.

como que los procesos se diseñen desde el inicio de acuerdo con los principios de protección de datos personales.

Ana Garriga Domínguez
Área de Filosofía do Dereito
Escola Superior de Enxeñaría Informática
Universidade de Vigo
Campus de Ourense
32004 Ourense
e-mail: agarriga@uvigo.es

ISSN: 1133-0937
DOI: 10.14679/1058